HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200300133-2

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Michael John Wray	Confirmation No.:	8240
Application No.:	10/810,348	Examiner:	Kristin D. Sandoval
Filing Date:	March 26, 2004	Group Art Unit:	2132

Title: Security Attributes...

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on July 8, 2008.

☒ The fee for filing this Appeal Brief is $510.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $460	☐ 3rd Month $1050	☐ 4th Month $1640

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 510. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Ladas & Parry LLP

By /Richard P. Berg/

Richard P. Berg

Attorney/Agent for Applicant(s)

Reg No. : 28,145

Date : September 8, 2008

Telephone : 323 934 2300

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Michael John Wray	) On Appeal to the) Board of Appeals
Patent Application No.: 10/810,348	)
Filed: 26 March 2004	) Group Art Unit: 2132)
	) Examiner: Sandoval, K. D
For: "Security attributes of nodes in trusted computing systems"	) Date: September 8, 2008

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final Rejection, dated April 8, 2008, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed on September 9, 2008, because the Notice of Appeal was filed on April 8, 2008 and September 8, 2008 fell on a Sunday. Please charge the Appeal Brief fee of $510.00 to deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC

RELATED APPEALS AND INTERFERENCES

Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-8, 10 and 11 are present in the application. Claims 9 and 12 have been canceled without prejudice. Claims 1-8, 10 and 11 are the subject of this Appeal and are reproduced in the accompanying Claims appendix.

STATUS OF AMENDMENTS

No claim amendments have been proffered in response to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates to a system and method for resolving a rule conflict within a security policy applied to a trusted computing platform, wherein the fileset to which each of the conflicting rules v and s refers (or "scope") is determined (step 10). It is then determined (at step 12) if the scope of one of the rules s is a complete subset of the scope of rule r. If so, rule s is applied to the accessed file f (at step 14). If not, the conflict is resolved in another way, for example, by determining the most restrictive of rules r and s (at step 16) and applying the result accordingly (step 18). [Abstract; Figures 1, 2, & 7-9; p. 5, l. 11 - p. 6, l. 25; p. 7, l. 21 through p. 9, l. 19; and p. 12, l. 12 through p. 14, l. 11].

Claim 1 is directed to a system comprising a trusted computing platform [element 10; p. 7, l. 21 through p. 8, l. 17], one or more logically protected computing environments [p. 9, ll. 11-14] and a filesystem comprising a plurality of files and links defining access paths between said files [Figure 8; p. 7, ll. 12-13] the system being arranged to load onto said trusted computing platform a predetermined security policy [p. 5, ll. 11-22] including a plurality of security rules in respect of one or more of said logically protected computing environments and/or said files [p. 5, ll. 11-22], the system being further arranged to:

(1) determine that first and second security rules apply to a specified file or set of files [Figure 9, step 10; p. 5, ll. 11-22; p. 13, ll. 10-19],

(2) determine the complete set of files, or fileset, to which each of said first and second security rules applies [p. 5, ll. 11-22],

(3) determine if the fileset of said first security rule is a complete subset of the fileset of said second security rule [Figure 9, step 12; p. 5, ll. 11-22; p. 13, ll. 10-19], and if so,

a. applying said first security rule to said specified file or set of files, and otherwise [Figure 9, step 14; p. 5, ll. 11-22; p. 13, ll. 10-19],

b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of files [Figure 9, steps 16 & 18; p. 5, ll. 11-22; p. 13, ll. 10-19].

Claim 10 is directed to a method of applying a predetermined security policy [p. 5, ll. 11-22] to a system having trusted computing platform [element 10; p. 7, l. 21 through p. 8, l. 17], one or more logically protected computing environments [p. 9, ll. 11-14] and a filesystem [Figure 8; p. 7, ll. 12-13] comprising a plurality of files and links defining access paths between said files, said security computing environments and/or said files, the method carried out by the system comprising the steps of: determining that first and

second security rules apply to a specified file or set of files [Figure 9, step 10; p. 5, ll. 11-22; p. 13, ll. 10-19], determining the complete set of files, or fileset, to which each of said first and second security rules applies [p. 5, ll. 11-22], determining if the fileset of said first security rule is a complete subset of the fileset of said second security rule [Figure 9, step 12; p. 5, ll. 11-22; p. 13, ll. 10-19], and if so,

a. applying said first security rule to said specified file or set of files, and otherwise [Figure 9, step 14; p. 5, ll. 11-22; p. 13, ll. 10-19],

b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of files [Figure 9, steps 16 & 18; p. 5, ll. 11-22; p. 13, ll. 10-19].

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue: Whether Claims 1-8 and 10-11 are patentable under 35 U.S.C. 102(e) in view of Austel, U.S. Patent No.6,430,561, (hereinafter "Austel")?

ARGUMENT

Issue: Whether Claims 1-8 and 10-11 are patentable under 35 U.S.C. 102(e) in view of Austel, U.S. Patent No.6,430,561, (hereinafter "Austel")?

In the final Office Action of April 8, 2008, the Examiner rejects each pending claims, namely, claims 1-8 and 10-11 under 35 U.S.C. §102(e) as being anticipated by Austel. Appellants respectfully disagree.

Appellants submit that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP 2131 quoting *Verdegaal Bros. V. Union Oil Co, of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The Examiner is also reminded that "[the] identical invention must be shown in as complete detail as is contained in the ... claim." MPEP 2131 quoting *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Appellants submit that the Examiner has not shown that Austel teaches each and every element as set forth in the rejected claims. In particular:

Claim 1

Appellants submit that the Examiner has not shown that Austel teaches, *inter alia*, the following features recited by Claim 1 of the present application:

(1) "a trusted computing platform, one or more logically protected computing environments"

As is explained in applicant's application at page 2, starting at line 13:

> "In the applicant's co-pending disclosure WO 00/48063, incorporated herein by reference, there is disclosed the concept of a `trusted computing platform' comprising a computing platform which has a `trusted component' in the form of a built-in hardware and software component. This document describes the use of a Trusted Device (TD) or Trusted Platform Module (TPM) to enable verification of the integrity of computing apparatus by the reliable measurement and reporting of integrity metrics. A TD/TPM conforms to the Trusted Computing Platform Alliance (TCPA) specification, see for example www.trustedpc.org.
>
> "A Trusted Device or Trusted Platform Module may include one or more logically protected computing environments or 'compartments' within which a service or process may be run. The actions or privileges within a

> compartment are constrained, particularly to restrict the ability of a process to execute methods and operations which have effect outside the compartment, such as methods that request network access or access to files outside of the compartment. Also, operation of a process or service within a compartment is performed with a high level of isolation from interference and prying by outside influences. The or each compartment may be an operating system compartment controlled by an operating system kernel. This is also referred to as a compartmented operating system or a trusted operating system.
>
> "Trusted operating systems have been available for several years in a form designed for handling and processing classified (military) information, using a containment mechanism enforced by a kernel of the operating system with mandatory access controls to resources of the computing platform such as files, processes and network connections. The operating system attaches labels to the resources and enforces a security policy which governs the allowed interaction between these resources based on their label values. Many trusted operating systems apply a security policy based on the Bell-Lapadula model discussed in the paper 'Applying Military Grade Security to the Internet' by C I Dalton and J F Griffin published in Computer Networks and ISDN Systems 29 (1997) 1799-1808."

While a trusted computing platform is, *per se*, well known in the art, Austel does not teach a "trusted computed platform" nor does Austel mention "one or more logically protected computing environments". The term "trusted computing platform" is well known in the prior art and applicant's specification clearly sets forth the meaning of the term.

The Applicant has admitted that these elements are known, *per se*, in the prior art. However, this rejection is an anticipation rejection under 35 USC 102, and the Examiner should not be permitted to make what is in essence an obviousness type rejection and parade it as an anticipation rejection. If it is obvious to combine a trusted computing platform prior art reference with Austel, then the

Examiner should be required to make the necessary showings and not just ignore these limitations.

(2) "(2) determine the complete set of files, or fileset, to which each of said first and second security rules applies,"

This limitation of claim 1 is not specifically addressed in the rejection, but it is noted that the Examiner makes a blanket rejection of this and other language of claim 1, referring the applicant to col. 6, line 42 through col. 7, line 25 of Austel. Since Austel does not meet this limitation, the anticipate rejection is improper. If the Examiner thinks that it would be obvious to modify Austel to meet this limitation, then he needs to be making an obviousness type rejection, not an anticipation rejection.

(3) "(3) determine if the fileset of said first security rule is a complete subset of the fileset of said second security rule, and if so,

a. applying said first security rule to said specified file or set of files, and otherwise,

b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of file." [Emphasis added]

The security rules of Austel are related to military security, such as "top secret", "secret" and "confidential". The Examiner has noted to Applicant that from an access viewpoint, that a computer which has access to "top secret" files, also has access to "secret" and "confidential" files and therefore the first security rule of claim 1 can be read on the "secret" rule and that the second security rule of claim 1 can be read on the "top secret" rule.

The final rejection is not clear at all on the points made immediately above, so the Applicant's understanding of the Examiner's rationale for rejecting claim 1 comes from a telephone call which the undersigned had with the Examiner. If the Board of Appeals focuses on the written rationale provided by the Examiner, it will be quickly noted that the Examiner gives short shrift to the limitations of claim 1 and apparently expects the Board of Appeals to work out for itself which limitations of claim 1 allegedly read on what disclosure of Austel.

Based upon the Applicant's understanding of the Examiner's construction of Austel, the applicant has pointed out that that the Examiner's construction of the prior art reference (so far as Applicant understands it) does not meet the "otherwise, b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of file" limitation of claim 1.

The Examiner disagrees asserting that the fact that "as system administrator, computer system A may modify (e.g. upgrade or downgrade) the secrecy access of a file". See the "response to arguments" portion of the final rejection.

Even if a computer can modify the secrecy access of a file, this facility does not meet the claim limitation. The claim language in question says "determine if the fileset of said first security rule is a complete subset of the fileset of said second security rule" and "if so" then apply the rule of subparagraph (a) "otherwise apply rule of subparagraph (b).

According to the Applicant's understanding of the Examiner's position, the first security rule of claim 1 can be read on the "secret" rule of Austel while the second

security rule of claim 1 can be read on the "top secret" rule of Austel. So Austel then applies the first rule. Manually changing the security access level of a particular file doesn't change the outcome of this test. "Secret" is still a subset of "top secret" no matter what anyone does to a the security level of a given file. The Examiner simply misreads the clear claim language of claim 1.

The Examiner does not look at the reverse situation, namely, if you assume that the first security rule of claim 1 is read on the "top secret" rule of Austel while the second security rule of claim 1 is read on the "secret" rule of Austel, then at least the otherwise clause of claim 1 is triggered. But the claim language says that the "otherwise" situation gives rise to "selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of file". That does not happen in Austel. If a computer has "top secret" access it can open "top secret", "secret" or "confidential" files (subparagraph a of the test). If a computer has only "secret" access it can only open "secret" and "confidential" files (which does no meet subparagraph b of the test). In this latter "otherwise" situation, only the second rule of Austel can be applied and the first rule (top secret) of Austel is never applied! The limitation "otherwise, b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of file" just does not occur in Austel. Austel will always apply the second rule!

Furthermore, even in the process of misreading the claim language, the Examiner has not shown any disclosure of "selecting one of said first and second security rules on the basis of another attribute thereof". Austel mentions that the security level of a given file can be changed, but based on what "attribute thereof"? So even if one accepts the Examiner's misconstruction of claim 1, the limitation "selecting one of said first and

second security rules on the basis of another attribute thereof" is still not met nor is this limitation discussed in any meaningful way in the final rejection.

Summary: Claim 1

The Examiner has failed to demonstrate how Austel allegedly anticipates each and every limitation of claim 1. Even if the Examiner could come up with a suitable rationale for overcoming the points made above relative to features 1 and 2 made above (by citing additional art and making a rejection based on obviousness instead of anticipation), this is not a point which this Board of Appeals need dwell on given the fact the third point above relative to feature 3 with respect to the "otherwise" clause has claim language which not only does Austel fail to teach, but which Austel teaches away from.

Claim 5

Claim 5 recites "A system according to claim 3, wherein said first and second security rules are execution control rules and the fileset to which said first security rule applies is not a complete subset of the fileset to which said second security rule applies, the system is arranged to select and apply the rule which was most recently added to the security policy."

The Examiner points to a paragraph in Austel at col. 10, lines 10-21, which contains a discussion of a guard program.

While that discussion may be interesting, it fails to address the claim language of claim 5 recited above, most particularly, the limitation "to select and apply the rule which was most recently added to the security policy".

Claim 6

Claim 6 recites "a system according to claim 5, arranged to provide a warning or error message indicating to a user that a rule conflict exists."

The Examiner points to paragraphs in Austel at col. 9, lines 4-22 and col. 10, line 59 through col. 11, line 7, which include a discussion of chain execute permission and mandatory versus permissive access rights. But there is no discussion of "a rule conflict" nor is there any discussion of a "warning or error message". The cited paragraphs do not meet claim 6.

Austel is talking about access rules at the cited paragraphs at col. 9. Austel is not dealing with "a rule conflict" as recited by claim 6.

Claim 7

Claim 7 recites "means for identifying the creation of a rule conflict when a link between files or sets of files is created and providing an error message or warning accordingly."

The Examiner points to paragraphs in Austel at col. 9, lines 4-22 and col. 10, line 59 through col. 11, line 7, which include a discussion of chain execute permission and mandatory versus permissive access rights. But there is no discussion of "means for

identifying the creation of a rule conflict when a link between files or sets of files is created" nor is there any discussion of an " error or warning message". The cited paragraphs do not meet claim 7.

Austel is talking about access rules at the cited paragraphs at col. 9. Austel is not dealing with "a rule conflict" as recited by claim 7.

Claim 8

Claim 8 recites "a system according to claim 7, arranged to remove the offending link to remove the conflict."

The Examiner points to paragraphs in Austel at col. 9, lines 4-22 and col. 10, line 59 through col. 11, line 7, which contain a discussion of chain execute permission and mandatory versus permissive access rights. But there is no discussion of the system being arranged to "to remove the offending link to remove the conflict". The cited paragraphs do not meet claim 7.

Claim 10

Claim 10 recites a "method of applying a predetermined security policy to a system having trusted computing platform, one or more logically protected computing environments and a filesystem comprising a plurality of files and links defining access paths between said files, said security computing environments and/or said files, the method carried out by the system comprising the steps of:

determining that first and second security rules apply to a specified file or set of files,

determining the complete set of files, or fileset, to which each of said first and second security rules applies,

determining if the fileset of said first security rule is a complete subset of the fileset of said second security rule, and if so,

a. applying said first security rule to said specified file or set of files, and otherwise,

b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of files."

Claim 10 includes essentially the same features discussed above with reference to claim 1 which the Examiner's rejection fails to address. As such Austel, fails to teach "a system having trusted computing platform, one or more logically protected computing environments" (feature 1); or "determining the complete set of files, or fileset, to which each of said first and second security rules applies" (feature 2) for the reasons discussed above.

Most importantly Austel fails to teach: "determining if the fileset of said first security rule is a complete subset of the fileset of said second security rule, and if so, a. applying said first security rule to said specified file or set of files, and otherwise, b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of files" as discussed above with reference to claim 1.

Claims 2-4 and 11

Claims 2-4 and 11, at least based on their dependency on Claims 1 or 10, are also patentable over Austel and the rejection of same should be overturned on appeal.

Conclusion

For the extensive reasons advanced above, Appellants respectfully contend that each rejected claim is patentable over Austel. Therefore, reversal of all rejections is courteously requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this document is being transmitted to the Patent and Trademark Office via electronic filing.

September 8, 2008
(Date of Transmission)

Lonnie Louie
(Name of Person Transmitting)

/Lonnie Louie/
(Signature)

/Richard P. Berg 28,145/
Richard P. Berg
Attorney for Appellants
Reg. No. 28,145
LADAS & PARRY LLP
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300

Enclosures - Claims Appendix
Evidence Appendix
Related Proceedings Appendix

1. A system comprising

a trusted computing platform,

one or more logically protected computing environments and

a filesystem comprising a plurality of files and links defining access paths between said files,

the system being arranged to load onto said trusted computing platform a predetermined security policy including a plurality of security rules in respect of one or more of said logically protected computing environments and/or said files,

the system being further arranged to:

(1) determine that first and second security rules apply to a specified file or set of files,

(2) determine the complete set of files, or fileset, to which each of said first and second security rules applies,

(3) determine if the fileset of said first security rule is a complete subset of the fileset of said second security rule, and if so,

a. applying said first security rule to said specified file or set of files, and otherwise,

b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of files.

2. A system according to claim 1, wherein said security rules comprise or include a plurality of file rules defining discretionary access controls in respect of one or more of said logically protected computing environments and/or files.

3. A system according to claim 1, wherein said security rules comprise or include a plurality of execution control rules defining or modifying security attributes in respect of one or more of said logically protected computing environments and/or files.

4. A system according to claim 2, wherein in said first and second security rules are file rules, and the fileset to which said first security rule applies is not a complete subset of the fileset to which the second security rules applies, the system is arranged to determine which of the first and second security rules is the most restrictive, and apply that rule to said specified file or set of files.

5. A system according to claim 3, wherein said first and second security rules are execution control rules and the fileset to which said first security rule applies is not a complete subset of the fileset to which said second security rule applies, the system is arranged to select and apply the rule which was most recently added to the security policy.

6. A system according to claim 5, arranged to provide a warning or error message indicating to a user that a rule conflict exists.

7. A system according to claim 1, including means for identifying the creation of a rule conflict when a link between files or sets of files is created and providing an error message or warning accordingly.

8. A system according to claim 7, arranged to remove the offending link to remove the conflict.

10. A method of applying a predetermined security policy to a system having trusted computing platform, one or more logically protected computing environments and a filesystem comprising a plurality of files and links defining access paths between said files, said security computing environments and/or said files, the method carried out by the system comprising the steps of:

determining that first and second security rules apply to a specified file or set of files,

determining the complete set of files, or fileset, to which each of said first and second security rules applies,

determining if the fileset of said first security rule is a complete subset of the fileset of said second security rule, and if so,

a. applying said first security rule to said specified file or set of files, and otherwise,

b. selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of files.

11. A method according to claim 10 wherein the security rules define access controls and/or modify security attributes.

No evidence is being submitted

There are no related proceedings.